

UNITED STATES DISTRICT COURT

for the
District of OregonIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)2 Subject Devices
as described in attachments A-1 & A-2

Case No. 3:20-mc-00273 A-B

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

2 Subject Devices as described in attachments A-1 & A-2 hereto.

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B-1 & B-2 hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C 841 (a)(1) and 846	Possession and Conspiracy to Possess with Intent to Distribute Methamphetamine

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Zachary Wills, DEA Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone at 1:55 a.m./p.m. (specify reliable electronic means).

Date: 03/24/2020



Judge's signature

City and state: Portland, Oregon

Hon. Youlee Yim You, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF ZACHARY WILLS

**Affidavit in Support of an Application
Under Rule 41 for a Search Warrant**

I, Zachary Wills, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Drug Enforcement Administration (“DEA”) and have been since September 2016. I am currently assigned to the DEA Portland District Office. My duties include conducting criminal investigations for possible violations of federal law, particularly those found in Title 18 and Title 21 of the United States Code. I have received specialized training from the DEA, including a 19-week Basic Agent Training course. Prior to joining DEA, I was a Police Officer with the Metropolitan Police Department in Washington D.C. for approximately three years. During my tenure with the police department, I worked as a district patrol officer and in the Narcotic Special Investigation Division—Gun Recovery Unit.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the search and examination of the following two devices (hereinafter “**Subject Devices**”):

- a. Exhibit N-28 – Silver iPhone: call number (818) 456-8816 with International Mobile Equipment Identification (IMEI) number 353341074972994 (“**Subject Device 1**”);
- b. Exhibit N-30 – Gray iPhone: call number (971) 888-2187 with International Mobile Equipment Identification (IMEI) number: 354848093614745 (“**Subject Device 2**”);

which were seized by the DEA on March 10, 2020, and are currently logged into the non-drug evidence vault located at the DEA Portland District Office: 100 SW Main Street, Suite 500, Portland, Oregon, as described in Attachment A1-A2 hereto, and the extraction of electronically stored information from the **Subject Devices**, as described in Attachment B1-B2 hereto. As set forth below, I have probable cause to believe and do believe that the **Subject Devices** constitute evidence, fruits, and instrumentalities of violations of Title 21 of the United States Code, Sections 841(a)(1) and 846.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 21, U.S.C., §§ 841(a)(1) and 846, Possession with the Intent to Distribute a Controlled Substance and Conspiracy to Possess with the Intent to Distribute a Controlled Substance, make it illegal to possess with intent to distribute a Controlled Substance, or to conspire to do so.

Statement of Probable Cause

11. On March 10, 2020, investigators used a cooperating defendant (CD) to place a call to “Eric,” subsequently identified as Eric Barajas and the user of (818) 456-8816 (“**Subject Device**

1”), in order to arrange a purchase of heroin and methamphetamine to transpire later that day. Investigators observed in the CD’s phone the saved contact associated with the phone number for **Subject Device 1** named as “Eric Jr.” The calls were not recorded, but all calls were placed in the immediate presence of, and at the instruction of, investigators. During the call, investigators heard Eric Barajas agree to meet with the CD at 5:00 p.m. in order to provide the heroin. Additionally, Eric Barajas told the CD that “Junior” would be calling the CD momentarily.

12. Following the initial call, the CD received a call from (971) 888-2187 (“**Subject Device 2**”). The user of the phone identified himself as “Junior,” subsequently identified as Elias Arellano. During the call, investigators heard Elias Arellano state “we,” meaning Elias Arellano was referring to himself as well as another person accompanying him, who investigators believed to be Eric Barajas. Elias Arellano went on to tell the CD, we need to go pick up the “tires, if you know what I mean.” Through training and experience, including knowledge that drug traffickers often use coded or cryptic language to refer to drugs, as well as the CD’s *controlled* intention to buy heroin from Elias Arellano, investigators believed Elias Arellano actually meant that he and Eric Barajas needed to pick up the heroin (i.e. tires).

13. Following the call, investigators conducted a law enforcement database check and located a booking photo for Elias Arellano. The CD positively identified Elias Arellano as the individual s/he knows to be “Junior.”

14. At approximately 5:57 p.m., the CD received a text message from **Subject Device 2** stating, “On our way he had to come back to get what he said.” Following additional calls with **Subject Device 1**, Eric Barajas directed the CD to travel to the Space Age Fuel on “174th and

Foster” to conduct the purchase. At approximately 6:25 p.m., investigators established physical surveillance in the vicinity of the Space Age Fuel – 16431 SE Foster Road, Gresham, Oregon.

15. At approximately 6:30 p.m., investigators identified a blue Toyota Tacoma backing into the parking lot of M&M Tires – 6612 SE Jenne Road, Portland, Oregon. The M&M Tire shop is directly north of the Space Age Fuel gas station. Investigators identified Eric Barajas to be the driver and Elias Arellano to be the passenger. Shortly after Elias Arellano and Eric Barajas exited the vehicle, investigators observed Eric Barajas walking from the M&M Tires towards the Space Age Fuel. Investigators placed one additional call to **Subject Device 1** and observed Eric Barajas answering the phone. After that observation, investigators from another unit attempted to arrest Eric Barajas who subsequently fled on foot. Eric Barajas was detained after a brief foot chase. Investigators could hear Eric Barajas running in the background as well as law enforcement giving Eric Barajas commands to stop running. Investigators subsequently seized **Subject Device 1**, along with an additional phone, from Eric Barajas. Simultaneously, investigators observed Elias Arellano walk into the inside of the M&M Tires. Investigators believe Elias Arellano threw two cellphones and the Toyota Tacoma keys on a table, before hiding in the rear of the M&M Tire shop. Investigators subsequently seized **Subject Device 2**, along with an additional device, located on the table.

16. A search incident to arrest revealed Eric Barajas was in possession of a brown paper bag containing three individually packaged plastic bags of suspected heroin weighing approximately 554.1 gross gram weight (ggw), which included packaging materials.

17. A search of the blue Toyota Tacoma revealed a black backpack containing additional suspected heroin weighing approximately 140.3 ggw, including the packaging materials

that contained the suspected heroin. The contents of the suspected heroin were not field tested due to officer safety. Based on my training and experience, I believe the suspected heroin is in fact heroin.

18. Investigators subsequently transported Eric Barajas and Elias Arellano back to the Portland DEA office in order to conduct interviews. At the start of the interview, I read Eric Barajas his Miranda Rights, via a DEA-13a Miranda Card. Eric Barajas advised he wanted his attorney present during questioning and the interview concluded at that time. At the start of the interview for Elias Arellano, I read his Miranda Rights, via a DEA-13a Miranda Card. Elias Arellano stated he understood his rights and was willing to speak with investigators. Elias Arellano stated they were on their way to pick up cash and sell drugs to an individual located at the Space Age Fuel station. Elias Arellano stated he had no involvement to the sale of the drugs and Eric Barajas would be the individual delivering the drugs. Elias Arellano stated he was unaware of what drugs Eric Barajas would be delivering nor did he know how much cash Eric Barajas would be picking up. When asked if he has any aliases, Elias Arellano stated he is also known as “Junior.”

19. I know from training and experience that drug traffickers use cellular telephones and electronic devices to communicate with other DTO members. I also know that drug traffickers often utilize multiple cellular devices to discuss drug trafficking activities in an effort to avoid law enforcement detection by compartmentalizing their communications with drug customers from communications with other DTO members.

20. Based on investigators communicating with Elias Arellano and Eric Barajas on two different phones, I believe the **Subject Devices** currently in possession of DEA were used to

facilitate the delivery of suspected heroin. Based on the information above, I believe the **Subject Devices** contain evidence of a conspiracy to distribute heroin in violation of Title 21 United States Code Sections 843(b) and 846.

21. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet,¹ including the use of apps.² Wireless telephones may also include a global positioning system (“GPS”) technology for determining the location of the device.

22. Based on my training, experience, and research, I know that **Subject Devices** have capabilities that allow them to serve as wireless telephones, digital cameras, portable media

¹ The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

² Apps is an abbreviation for applications. An app is a self-contained program or piece of software designed to fulfill a particular purpose. An app can run on the Internet, on a computer, on a cell phone, or on other electronic devices.

player, and GPS navigation device. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

23. As further described in Attachments B-1 through B-2 this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how **Subject Devices** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on **Subject Devices** because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, **Subject Devices** may contain electronic evidence of how they were used, what they has been used for, and who used them. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Data on **Subject Devices** can provide evidence of a file that was once on **Subject Devices** but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on **Subject Devices** that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on **Subject Devices** that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times **Subject Devices** were in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

f. A person with appropriate familiarity with how **Subject Devices** work may, after examining this forensic evidence in its proper context, be able to draw conclusions about how **Subject Devices** were used, the purpose of their use, who used them, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on **Subject Devices** is evidence may depend on other information stored on **Subject Devices** and the

application of knowledge about how **Subject Devices** function. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how **Subject Devices** were used, the purpose of their use, who used them, and when, the examiner may have to establish that a particular thing is not present on **Subject Devices**.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of **Subject Devices** consistent with the warrant. The examination may require authorities to employ techniques, including imaging **Subject Devices** and computer-assisted scans and searches of the entirety of each of **Subject Devices** that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

25. The initial examination of **Subject Devices** will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

26. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on **Subject Devices** or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data

falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

27. If an examination is conducted, and it is determined that **Subject Devices** do not contain any data falling within the ambit of the warrant, the government will return **Subject Devices** to their respective owners within a reasonable period of time following the search and will seal any image of **Subject Devices**, absent further authorization from the Court.

28. The government may retain **Subject Devices** as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against **Subject Devices** and/or the data contained therein.

29. The government will retain a forensic image of **Subject Devices** for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

///

///

Conclusion

31. Based on the foregoing, I have probable cause to believe, and I do believe, that Subject Devices described in Attachments A-1 through A-2 contains evidence of the Target Offenses, as set forth in Attachments B-1 through B-2. I therefore request that the Court issue a warrant authorizing a search of Subject Devices described in Attachment A-1 through A-2 for the items listed in Attachments B-1 through B-2 and the seizure and examination of any such items found.

32. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Sarah Barr, and AUSA Barr advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Request for Sealing

33. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may endanger the life or physical safety of an individual, cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an investigation.


///

///

Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

By Phone
ZACHARY WILLS
DEA Special Agent

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 1:55
p.m. on March 24, 2020.


HONORABLE YOULEE YIM YOU
United States Magistrate Judge

ATTACHMENT A-1

Phone to Be Searched

The phone to be searched is a Silver iPhone, with call number call number (818) 456-8816 and International Mobile Equipment Identity (“IMEI”) number 353341074972994 (hereinafter “Subject Device 1”), and is currently located in secure storage at the DEA located at 100 SW Main St Ste 500, Portland, Oregon 97204.

ATTACHMENT A-2

Phone to Be Searched

The phone to be searched is a Gray iPhone, with call number (971) 888-2187 and International Mobile Equipment Identity (“IMEI”) number 354848093614745 (hereinafter “Subject Device 2”), and is currently located in secure storage at the DEA located at 100 SW Main St Ste 500, Portland, Oregon 97204.

ATTACHMENT B-1

Items to Be Seized

1. All records on the Device described in Attachment A-1 that relate to violations of 21, U.S.C., §§ 841(a)(1) and 846, Possession with the Intent to Distribute a Controlled Substance and Conspiracy to Possess with the Intent to Distribute a Controlled Substance, and 21, U.S.C., § 843(b), and Use of a Communication Facility to Distribute a Controlled Substance (hereinafter “Target Offenses”), including:

- a. Lists of customers and related identifying information.
- b. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.
- c. Information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).
- d. Information recording the Device’s schedule or travel from January 1, 2019 to the present.
- e. Bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

- a. Records of Internet Protocol addresses used.
- b. Records of Internet activity, including firewall logs, caches, browser

history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

ATTACHMENT B-2

Items to Be Seized

1. All records on the Device described in Attachment A-2 that relate to violations of 21, U.S.C., §§ 841(a)(1) and 846, Possession with the Intent to Distribute a Controlled Substance and Conspiracy to Possess with the Intent to Distribute a Controlled Substance, and 21, U.S.C., § 843(b), and Use of a Communication Facility to Distribute a Controlled Substance (hereinafter “Target Offenses”), including:

- a. Lists of customers and related identifying information.
- b. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.
- c. Information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).
- d. Information recording the Device’s schedule or travel from January 1, 2019 to the present.
- e. Bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

- a. Records of Internet Protocol addresses used.
- b. Records of Internet activity, including firewall logs, caches, browser

history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.